

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日 2 0 0 3 年 7 月 2 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 8 9 9 2 4
Application Number:

[ST. 10/C] : [J P 2 0 0 3 - 1 8 9 9 2 4]

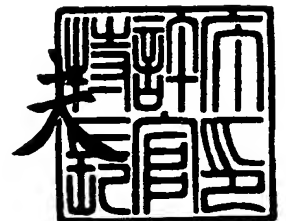
出 願 人 キヤノン株式会社
Applicant(s):

CERTIFIED COPY OF
PRIORITY DOCUMENT

2 0 0 3 年 9 月 1 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 255274

【提出日】 平成15年 7月 2日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 13/00

【発明の名称】 サーバ装置

【請求項の数】 18

【発明者】

 【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社
社内

 【氏名】 明星 俊彦

【発明者】

 【住所又は居所】 東京都大田区下丸子 3 丁目 3 0 番 2 号 キヤノン株式会社
社内

 【氏名】 山崎 信一

【特許出願人】

 【識別番号】 000001007

 【氏名又は名称】 キヤノン株式会社

【代理人】

 【識別番号】 100087446

 【弁理士】

 【氏名又は名称】 川久保 新一

【先の出願に基づく優先権主張】

 【出願番号】 特願2002-247899

 【出願日】 平成14年 8月28日

【手数料の表示】

 【予納台帳番号】 009634

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704186

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 サーバ装置

【特許請求の範囲】

【請求項 1】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置。

【請求項 2】 請求項 1 において、

上記複数の電子機器は、Bluetoothによって上記アクセスポイントと接続され、

上記参加者判別手段は、上記電子機器とアクセスポイントとの間の認証に用いたPINコードに基づいて、上記参加者の立場を判別することを特徴とするサーバ装置。

【請求項 3】 請求項 1 または請求項 2 において、

上記参加者判別手段は、会議の主催者と上記主催者以外の参加者とを判別する手段であり、

上記会議システムの管理サーバは、上記主催者と上記参加者との操作制限を行う操作制限テーブルを有することを特徴とするサーバ装置。

【請求項 4】 請求項 3 において、

上記操作制限テーブルで制限される項目は、他のネットワークへの接続制限の項目を含む項目であることを特徴とするサーバ装置。

【請求項 5】 請求項 4 において、

上記電子機器に、IPアドレスを割り当てると同時に、IPアドレステーブルを作成するIPアドレステーブル作成部を有することを特徴とするサーバ装置。

【請求項 6】 請求項 5 において、

上記IPアドレステーブル作成部が作成したIPアドレステーブルと、ネット

ワークに接続されたゲートウェイが持つ I P アドレステーブルとを、共有して記憶する I P アドレス記憶部を有することを特徴とするサーバ装置。

【請求項 7】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に、上記通信システムにおける機能制限を割り当てることを特徴とするサーバ装置。

【請求項 8】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする通信システム。

【請求項 9】 会議に参加するユーザによって操作される複数の電子機器と、上記電子機器との間で情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される通信システムのサーバ装置において、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置。

【請求項 1 0】 請求項 9 において、

上記認証手続きは、無線リンクプロトコルレベルによる認証とリンクレベルよりも高いプロトコルレベルによる認証によって構成される手順であることを特徴とするサーバ装置。

【請求項 1 1】 請求項 1 0 において、

上記認証手続きにおいて、無線リンクレベルによる認証では、リンク確立時に Bluetooth における P I N コードを照会して認証を行い、上位プロトコルレベルによる認証では、上記無線リンクレベルでの認証動作を省くことを特徴とするサーバ装置。

【請求項 1 2】 請求項 9 において、

上記認証手続きは、認証のプロトコルレベルに応じて、異なる手順によって認証操作を行わせ、この認証手順の方法に基づいて、参加者の立場を判別することを特徴とするサーバ装置。

【請求項 1 3】 請求項 9 において、

上記参加者判別手段は、会議の主催者と、他のネットワークへのアクセス権限を持たずしかも上記会議の主催者以外の参加者と、他のネットワークへのアクセス権限を持ちしかも上記会議の主催者以外の参加者とを判別する手段であることを特徴とするサーバ装置。

【請求項 1 4】 請求項 1 3 において、

上記参加者判別手段による判別に基づいて、電子機器への I P アドレスの割り当てを行うことを特徴とするサーバ装置。

【請求項 1 5】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を通じて接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続きを行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とするサーバ装置。

【請求項 1 6】 請求項 1 5 において、

上記認証情報は、B l u e t o o t h における P I N コードと、上位プロトコルとの認証で定められた認証情報であることを特徴とするサーバ装置。

【請求項 1 7】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を通じて接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおいて、

認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続きを行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とする通信システム。

【請求項 1 8】 アクセスポイントを有する通信システムのサーバ装置において、

上記アクセスポイントが無線通信機器を認証する際に用いた認証情報に基づいて、上記無線通信機器の上記通信システム内の機能制限を行うことを特徴とするサーバ装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、通信システム、通信装置に係り、たとえば、会議システムを用いた会議の参加者の立場の判断と、会議システムにおける機能制限の割り当てとに関する。

【0 0 0 2】

【従来の技術】

従来の会議では、紙ベースで発表資料を参加者全員に配布するので、資源が無駄であるという欠点がある。また、資料が人数分揃わない場合には、不足部数を慌ててコピーし、会議の進行を妨げるという欠点がある。

【0 0 0 3】

一方、近年は、発表者が、P C（パーソナルコンピュータ）やP D A（P e r s o n a l D i g i t a l A s s i s t a n t s）を、会議室に持ち込み、発表資料をプロジェクタで投影し、プレゼンテーションすることが一般である。さらに、発表者以外の参加者にも、紙ベースではなく、ネットワーク経由で、資料データを配布することによって、上記欠点を克服している。

【0 0 0 4】

しかし、参加者が多い会議で、全員がネットワークを使用すると、配線が複雑になるという新たな欠点が生じる。この新たな欠点を克服するために、B l u e t o o t h等の無線通信を用いた会議システムが考えられている。

【0 0 0 5】

B l u e t o o t h方式は、アドホックなマルチポイント接続を行うので、最大接続数が、8 機器、通信範囲が1 0 mのピコネットを構築し、通信することが

でき、通信速度に関しては、非同期通信において、下り 7 2 1 K b p s、上り 5 7 . 6 K b p s の通信を行うことができる。また、音声通信もサポートし、1 つのチャンネルで、音声とデータとを転送することができる等、多種多様なプラットフォームでの利用が期待されている。

【 0 0 0 6 】

上記 B l u e t o o t h 等の無線通信を用いた会議システムによって、配線の煩雑さは解消されるが、無線接続による外部からの不正アクセス、データの改ざん等セキュリティ面で、別の欠点が浮上している。

【 0 0 0 7 】

しかも、一度認証を通ると、資料のコピー、プリントアウト、データの上書き等については、B l u e t o o t h の認証レベルでは制限することができないという別の欠点がある。

【 0 0 0 8 】

上記別の欠点を克服するために、プライベート用の P I N コードとテンポラリ用の P I N コードとの 2 種類の P I N コードを、機器の利用形態によって使分けることによって、利便性とセキュリティレベルとを向上する方法が提案されている（たとえば、特許文献 1 参照）。また、会議中の権限を、各端末に指定し、機能を制限することが提案されている（たとえば、特許文献 2 参照）。

【 0 0 0 9 】

また、上記不正アクセス、データの改ざんの問題やアクセス制御の問題に対して、P o r t B a s e d N e t w o r k A c c e s s C o n t r o l 技術によってセキュリティ強化を目的とした標準化作業が進んでいる（たとえば、非特許文献 1 参照）。

【 0 0 1 0 】

【特許文献 1】

特開 2 0 0 1 - 3 1 2 4 7 2 号公報

【特許文献 2】

特開 2 0 0 1 - 3 3 1 4 3 1 号公報

【非特許文献 1】

IEEE 802.1x (Institute of Electrical and Electronic Engineers 802.1x)

【0011】

【発明が解決しようとする課題】

特許文献2記載の発明では、参加者の機器に権限を与える際に、会議システムのアプリケーション上から、各参加者がどの権限で会議に参加するかを特定するタブを選択し、選択したタブに応じた権限を設定する。

【0012】

しかし、このようにすると、参加者の手間がかかる上、任意に権限の設定を変更することができ、権限を故意に変えてデータを操作することも可能であるという問題がある。

【0013】

一方、非特許文献1記載の発明では、端末認証サーバとしてRADIUS (Remote Authentication Dial-In User Service) サーバを設置し、端末が会議システムへアクセスするに先立って、認証サーバとの間で電子証明書やパスワード等を用いて認証を行う方法をとっている。

【0014】

しかし、このような構成では、会議参加者は、IEEE 802.1xに対応したプログラムを有する端末のみでしか、会議に参加することができず、IEEE 802.1xが検討される以前の端末や、Bluetoothが多く実装されているPDA (Personal Digital Assistance) 等で、IEEE 802.1xに対応していない機器を持ち込んで会議に参加することができないという問題がある。

【0015】

本発明は、会議システム等のシステムに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる通信システムのサーバ装置を提供することを

目的とするものである。

【0 0 1 6】

【課題を解決するための手段】

本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置である。

【0 0 1 7】

また、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に、上記通信システムにおける機能制限を割り当てることを特徴とするサーバ装置である。

【0 0 1 8】

さらに、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記認証手続きを行った電子機器に対して上記会議システムにおける機能制限を割り当てることを特徴とする通信システムである。

【0 0 1 9】

そして、本発明は、会議に参加するユーザによって操作される複数の電子機器と、上記電子機器との間で情報を送受信し、無線端末がネットワークに接続する際に必要なアクセスポイントが接続される通信システムのサーバ装置において、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装

置である。

【0020】

また、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続きを行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とするサーバ装置である。

【0021】

さらに、本発明は、会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおいて、認証手続きを行う手順と、認証手続きを行う際に用いる認証情報とに基づいて、上記認証手続きを行った電子機器に、上記会議システムにおける機能制限を割り当てることを特徴とする通信システムである。

【0022】

そして、本発明は、アクセスポイントを有する通信システムのサーバ装置において、上記アクセスポイントが無線通信機器を認証する際に用いた認証情報に基づいて、上記無線通信機器の上記通信システム内の機能制限を行うことを特徴とするサーバ装置である。

【0023】

【発明の実施の形態および実施例】

〔第1の実施例〕

図1は、本発明の第1の実施例である無線通信システムWC1を示すブロック図である。

【0024】

無線通信システムWC1は、会議システム管理サーバ10と、アクセスポイント20と、ゲートウェイ30と、PC40と、LAN50と、広域ネットワーク

60を有する。

【0025】

会議システム管理サーバ10は、広域ネットワーク60へアクセスするために必要であり、会議システムのアプリケーションを動作させるサーバである。

【0026】

PC40は、会議主催者や参加者が持参した無線端末の例であり、Bluetoothによる無線接続が可能である。

【0027】

アクセスポイント20は、無線端末としてのPC40から、根幹のLAN50に接続する際に必要となるポイントである。また、アクセスポイント20は、根幹のLAN50に接続され、一般的なスイッチングハブのような役目をする。会議主催者や参加者が持参したPC40を有線で会議サーバ10に接続する場合、ハブを用いて、会議システム管理サーバ10に複数台接続することができるが、無線接続する場合は、各機器をアクセスポイント20に接続し、アクセスポイント20経由で、会議システム管理サーバ10との間で、データをやりとりする。

【0028】

アクセスポイント20へ接続する場合、セキュリティを考慮し、ユーザ認証する必要がある。一般的に、PINコード(Personal Identification Number)を、機器間で交換することによって、ユーザ認証するが、アクセスポイント20のデフォルトPINコードが固定であると、一度接続したことがある人なら、同じPINコードを使って何度でも接続でき、セキュリティ面で問題がある。

【0029】

そこで、本実施例では会議の主催者が、デフォルトPINコードで、アクセスポイント20に予め接続し、会議の時にのみ有効なPINコードに変更する方法を採る。この場合、デフォルトPINコードが固定であると、上記のように、誰でも設定を変更できるので、デフォルトPINコードを故意に変更することもできる。すると、正規の主催者が、会議の時にのみ有効なPINコードに変更しようと考え、デフォルトPINコードで接続しようとしても、接続できないという

事態が生じる。

【 0 0 3 0 】

そこで、会議システム管理サーバ 1 0 によって運営される会議室予約システム等で会議室を予約した時に、その会議室付属のアクセスポイント 2 0 にデフォルト P I N コードが設定され、同時に、主催者にメール等で通知し、主催者は、会議システム管理サーバ 1 0 から通知された P I N コードを使ってアクセスポイント 2 0 に接続し、会議の時にのみ有効な P I N コードに変更する手段がとられている。参加者は、主催者から予め通知された会議の時にのみ有効な P I N コードを含む参加証を持って、会議室に臨み接続する。

【 0 0 3 1 】

図 2 は、本実施例における会議システム管理サーバ 1 0 を示すブロック図である。

【 0 0 3 2 】

会議システム管理サーバ 1 0 は、主制御部（C P U） 1 2 と、ネットワーク通信部 1 3 と、記憶部 1 4 と、データベース 1 5 と、入力部 1 6 と、表示部 1 7 と、テーブル作成部 1 8 と、判別部 1 9 とを有する。

【 0 0 3 3 】

主制御部 1 2 は、会議システム制御、各種アプリケーションの管理、入力部、表示部を制御する。

【 0 0 3 4 】

ネットワーク通信部 1 3 は、主制御部 1 2 の指示に従って、有線通信網、無線通信網に接続される各種無線端末としての P C 4 0 との間で、データを送受信する。記憶部 1 4 は、テーブル作成部 1 8 で作成された各種テーブルデータやファイル管理を行う。

【 0 0 3 5 】

入力部 1 6 は、キーボード、マウス等によって入力を制御し、表示部 1 7 は、C R T モニタ等の表示を制御する。テーブル作成部 1 8 は、I P アドレステーブルや機能制限テーブル等各種テーブルを作成する。判別部 1 9 は、ネットワーク通信部 1 3 が取得した参加証に基づいて、その参加証の送り主が会議の主催者で

あるか、参加者であるかを判別する。

【0 0 3 6】

図 3 は、本実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【0 0 3 7】

まず、会議の主催者は、会議室予約システム等で会議室を予約し（S 1）、アクセスポイント 2 0 に設定されているデフォルト P I N コードを使って、アクセスポイント 2 0 に接続し、会議の時にのみ有効な P I N コードに設定を変更する（S 2）。そして、その会議の時にのみ有効な P I N コードを、会議の参加者に電子メール等で通知する（S 3）。

【0 0 3 8】

次に、メールアドレス、P I N コード、社員 I D 等が記されている主催者用の参加証ファイルと、主催者以外の会議参加者用の参加証ファイルとを作成し（S 4）、この作成したファイルを、参加者全員にそれぞれ電子メール等で配布し（S 5）、会議に参加する（S 6）。なお、主催者用の参加証には、デフォルト P I N コードと、会議の時にのみ有効な P I N コードとの 2 つのコードが記述され、主催者以外の会議参加者の参加証には、会議の時にのみ有効な P I N コードのみが記述され、主催者以外の参加者には、主催者以外の会議参加者用の参加証ファイルを配布する。

【0 0 3 9】

図 4 は、本実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【0 0 4 0】

まず、主催者が配布した会議の時にのみ有効な P I N コードを、参加者が取得する（S 1 1）。この P I N コードの取得方法は、電子メールのみでなく、主催者が作成した W e b 等にアクセスし、主催者が配布した会議の時にのみ有効な P I N コードを取得するようにしてもよい。

【0 0 4 1】

次に、主催者が配布した参加証を、参加者が受け取り（S 1 2）、参加者はそ

の参加証を持参し、会議に参加する（S13）。この参加証には、PINコードが記載されているので、会議の時にのみ有効なPINコードを取得する処理（S11）を省くようにしてもよい。

【0042】

図5は、本実施例において、主催者がアクセスポイント20のPINコードを変更する処理を示すシーケンス図である。

【0043】

まず、主催者が会議室予約システムで会議室の予約を行うと、会議システム管理サーバ10は、LAN50経由でアクセスポイント20に接続し、アクセスポイント20に、デフォルトPINコードを設定する（S21）。この会議システム管理サーバ10は、会議室予約システムを運用し、会議室予約システムで会議室の予約が行われた際に、自動的にPINコードを作成し、このPINコードをデフォルトPINコードとしてアクセスポイント20に設定し、同時に、このデフォルトPINコードを予約者に通知するような機能を有する。

【0044】

主催者は、会議システム管理サーバ10からデフォルトPINコードの通知を受けると、このデフォルトPINコードと、会議の際に使用する会議の時にのみ有効なPINコードとを、無線機器としてのPC40に設定する。

【0045】

次に、主催者は、所有の無線機器としてのPC40から、アクセスポイント20に、接続要求を発行する（S22）。アクセスポイント20は、接続要求を受け、データが正しければ、接続確立のメッセージを、主催者のPC40に送信し、接続が確立する（S23）。

【0046】

その後に、アクセスポイント20は、主催者のPC40に認証要求を発行し、パスワードの要求を促す（S24）。主催者側のPC40は、認証要求を受けると、予め設定しておいたデフォルトPINコードを、アクセスポイント20に送信する（S25）。アクセスポイント20は、主催者のPC40から送られたPINコードが正しければ、主催者のPC40に認証完了を通知する（S26）。

【 0 0 4 7 】

次に、主催者の P C 4 0 は、P I N コードの設定変更要求を、アクセスポイント 2 0 に発行し（S 2 7）、これを受けたアクセスポイント 2 0 から、要求メッセージ受信応答が帰ってきたら（S 2 8）、予め設定しておいた会議の時にのみ有効な P I N コードを送信する（S 2 9）。アクセスポイント 2 0 は、新たな P I N コードを受信すると、その P I N コードに設定を変更し、変更完了のメッセージを、主催者の無線機器としての P C 4 0 に送信し、接続処理が完了する（S 3 0）。

【 0 0 4 8 】

なお、上記説明では、主催者の P C 4 0 からアクセスポイント 2 0 に送信するデフォルト P I N コードと、会議の時にのみ有効な P I N コードとは、自動的に送信されるが、アクセスポイント 2 0 からの要求に応じて、その都度、主催者が入力部（図示せず）を操作して入力し、上記入力された P I N コードを送信するようにしてもよい。

【 0 0 4 9 】

図 6 は、本実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【 0 0 5 0 】

なお、主催者が、図 5 で説明した P I N コードの設定を変更した後に、一度、アクセスポイント 2 0 との無線接続を切断し、再度、アクセスポイント 2 0 に接続する場合も、上記と同様の処理を行う。

【 0 0 5 1 】

参加者は、主催者から通知された会議の時にのみ有効な P I N コードを予め P C 4 0 に設定する。そして、会議室に着くと、所有の P C 4 0 から、アクセスポイント 2 0 に、接続要求を発行する（S 4 1）。アクセスポイント 2 0 は、接続要求を受け、データが正しければ、接続確立のメッセージを、参加者の P C 4 0 に送信し、接続が確立する（S 4 2）。

【 0 0 5 2 】

その後に、アクセスポイント 2 0 が、参加者の P C 4 0 に認証要求を発行し、

パスワードの要求を促す（S 4 3）。参加者の P C 4 0 は、認証要求を受けると、予め設定しておいた会議の時にのみ有効な P I N コードを送信する（S 4 4）。アクセスポイント 2 0 は、参加者の P C 4 0 から送られてきた P I N コードが正しければ認証完了のメッセージを送るので、参加者の P C 4 0 は、アクセスポイント 2 0 から認証完了のメッセージを受信したら（S 4 5）、アクセスポイント 2 0 を経由し、予め配布された参加証を、会議システム管理サーバ 1 0 に送信する（S 4 6）。会議システム管理サーバ 1 0 は、参加証を受信したら、図 7 で説明するような動作を行い、受信応答を参加者の P C 4 0 に送信し、接続処理が完了する（S 4 7）。

【0 0 5 3】

図 7 は、本実施例において、主催者または参加者から送られた参加証を受信した際に、会議システム管理サーバの判別部 1 9 の動作を示すフローチャートである。

【0 0 5 4】

参加証には、最低限、P I N コードが記述されていることを前提とする。

【0 0 5 5】

会議システム管理サーバ 1 0 は、図 6 のステップ S 4 6 で送信された参加証を受信すると、その参加証に記述されている P I N コードを確認する。参加証に記述されている P I N コードが 2 種類（デフォルト P I N コード、会議の時にのみ有効な P I N コード）であり（S 5 1）、しかも、会議システム管理サーバ 1 0 が保持している P I N コードと一致すれば（S 5 3）、接続相手を主催者と判別し、その参加証を送信した P C 4 0 に、主催者としての機能権限を与える（S 5 6）。

【0 0 5 6】

一方、P I N コードが 1 種類（会議の時にのみ有効な P I N コード）であり（S 5 1）、しかも、会議システム管理サーバ 1 0 が保持している P I N コードと一致すれば（S 5 2）、主催者以外の参加者であると判別し、その参加証を送ってきた P C 4 0 に、主催者以外の参加者としての機能権限を与える（S 5 4）。不正な P I N コードが記述された参加証を受信すれば、不正なアクセスとみなし

、そのPC40による全ての操作を不能にする（S55）。

【0057】

なお、上記説明では、接続完了後にPINコードが記述された参加証を転送する手順について記載したが、デフォルトPINコードを有しない参加者端末においては、接続時に、会議のときにのみ有効なPINコードを用いて接続するので、認証完了メッセージを受信した後の参加証転送を省くようにしてもよい。この場合、会議システム管理サーバ10では、この参加証を受信したときにのみ、接続相手を判定し、正しく2種類のPINコードを有している場合には、主催者としての機能権限を与える制御を行い、それ以外の場合には、参加者としての機能権限を与えるようにアクセス制御を行い、これによって、上記説明と同様の機能を実現し、さらに参加証転送手順を省くことができる。

【0058】

図8は、上記実施例において、会議システムによって制限される機能のテーブルを示す図である。

【0059】

図7のステップS56で主催者としての機能権限を与えられた場合は、図8に示す主催者の欄に丸印が記載されている機能を利用することができ、ステップS54で主催者以外の参加者としての権限が与えられた場合は、参加者の欄に丸印が記載されている機能を利用することができ、バツ印が記載されている機能を利用することができない。なお、三角印は、制限付きでその機能を利用できることを示す。

【0060】

ここで、図8に示す機能欄に記載されている「ファイルの閲覧」、「ファイルのコピー」、「ファイルの削除」、「ファイルの印刷」、「ファイル名変更」、「ファイルの上書き」は、図1に示すLAN50経由で他の機器に公開されているファイルを、それぞれ、閲覧、コピー、削除、印刷、名称変更、上書きすることである。

【0061】

「ファイルの保存」は、図1に示すLAN50経由で接続されるサーバ等の機

器（たとえば、会議システム管理サーバ10）にファイルを保存することである。「ネット閲覧」は、図1に示すゲートウェイ30を介して、広域ネットワーク60（インターネットやイントラネット）にアクセスする機能である。

【0062】

「IPアドレスの変更」は、アクセスポイント20に接続し、会議システム管理サーバ10から会議時の権限を与えられた際に、会議システム管理サーバ10が割り当てたIPアドレスを変更する機能である。「PINコードの変更」は、アクセスポイント20に設定されているPINコード（会議の時にのみ有効なPINコード）を変更する機能である。「メールの送受信」は、ゲートウェイ30を介して行う広域ネットワーク60とのメールの送受信機能である。

【0063】

[第2の実施例]

参加者それぞれに、外部アクセス可能なIPアドレスを割り当て、制限無しに広域ネットワーク60へアクセスすることができると、参加者がWebのメールサービス等で重要な情報を、故意に外部に漏らす可能性がある。

【0064】

そこで、本発明の第2の実施例は、第1の実施例の会議システム管理サーバ10が、PC40にIPアドレスを割り当てる方法を改良した実施例である。

【0065】

つまり、第2の実施例は、図6のステップS46で送信された参加証を受信した参加証に記述されているPINコードによって、会議システム管理サーバ10が、広域ネットワーク60へのアクセス制限をかける実施例である。

【0066】

具体的には、図7のステップS51において、PINコードが、2種類（デフォルトPINコード、会議の時にのみ有効なPINコード）であり、しかも、会議システムが記憶し、保持しているデフォルトPINコードが、会議の時にのみ有効なPINコードと一致すれば（S53）、その参加証を送信したPC40のユーザを主催者であると判別し、そのPC40の会議時の権限を、主催者として設定し、また、広域ネットワーク60へ接続できるIPアドレスを、そのPC4

0に割り当てる（S 5 6）。

【0 0 6 7】

P I Nコードが、1種類（会議の時にのみ有効なP I Nコード）であり、しかも、正しいP I Nコードであれば（S 5 1、S 5 2）、その参加証を送信したP C 4 0のユーザを、主催者以外の参加者であると判別し、そのP C 4 0の会議時の権限を、主催者以外の参加者として設定し、また、広域ネットワーク6 0へ接続できないI Pアドレスを割り当てる。会議システム管理サーバ1 0のI Pアドレスを取得する場合、L A N 5 0に接続されているゲートウェイ3 0が持つI Pアドレステーブルを取得し、共有することによって、会議システム管理サーバ1 0のI Pアドレスを取得する。

【0 0 6 8】

具体的には、無線端末としてのP C 4 0が、会議システム管理サーバ1 0に接続されたときに、会議システム管理サーバ1 0は、ゲートウェイ3 0が持つI Pアドレステーブルを取得する。これと同時に、会議システム管理サーバ1 0が取得する参加証に記載されているP I Nコードに基づいて、主催者であるか、参加者であるかを判別し、広域ネットワーク6 0へのアクセスを許可できる無線端末に対して、I Pアドレスを配布する。

【0 0 6 9】

今回は、ゲートウェイ3 0が持つI Pアドレステーブルの取得を、無線端末の接続と同時に行ったが、一定時間間隔でテーブルを取得するようにしてもよい。

【0 0 7 0】

また、取得したI Pアドレステーブルに、そのI Pアドレスを追加し、ゲートウェイ3 0に送信することによって、ゲートウェイ3 0と会議システム管理サーバ1 0とが、I Pアドレステーブルを共有する。

【0 0 7 1】

第2の実施例によれば、主催者と参加者とで、広域ネットワーク6 0へのアクセス制限をかけることによって、不正な外部アクセスを防ぐことができる。

【0 0 7 2】

[第3の実施例]

会議システム管理サーバ 10 では、参加者に与えるアクセス権限を、各無線端末としての PC 40 から入力される PIN コードに基づいて判定し、それぞれに IP アドレスを割り当てる。しかし、この場合、IEEE 802.1x のような上位プロトコルによる認証手順に対応している無線端末を有する参加者も、上位認証手順を使用することなく、無線リンクレベルでの認証を行う必要があり、機器のリソースを有効活用することができない。また、上位認証機能を会議システム管理サーバ 10 に持たせた場合、同参加者は、上位認証手順に加え、PIN コードによる認証も必要になり、煩雑な操作を強いることになる。

【0073】

本発明の第 3 の実施例は、会議システム管理サーバ 10 に、IEEE 802.1x 等の上位プロトコルによる認証機能を持たせ、同認証手順対応の無線端末による会議参加者と、非対応無線端末による会議参加者とが混在する場合に、各 PC 40 に有効な認証処理を行うアクセス制御に関する実施例である。

【0074】

具体的には、第 3 の実施例は、上記会議システム管理サーバ 10 に、上位認証機能（本実施例では IEEE 802.1x とする）を持たせ、アクセスポイント 20 において、PIN コードを要求するリンクレベルによる認証機能と、PIN コード入力を要求せずに無線端末との間におけるリンクレベルでの接続を許可し、リンクが確立した後に、上位認証手順を実行させる機能を持たせ、各認証結果に基づいて、アクセス権限を決定し、各無線端末としての PC 40 に、IP アドレスを割り当てる。

【0075】

図 9 は、本発明の第 3 の実施例における各無線端末の操作と、その操作に従った会議システム管理サーバ 10 の動作を示すフローチャートである。

【0076】

はじめに、会議システム管理サーバ 10 が運営する会議システムを、主催者が起動し（S61）、アクセスポイント 20 へリンク接続操作を行う。このログイン操作において、上記第 1、2 の実施例と同様に、デフォルト設定されている PIN コードを用いて、リンクレベルの認証を行うと、会議システム管理サーバ 1

0 が、ログイン端末を、主催者の P C 4 0 であると判断し、主催者権限によるアクセス権を与える I P アドレスを、同 P C 4 0 に割り当てる（S 6 2）。

【0 0 7 7】

I P アドレスの割り当てを受け、ログイン動作が完了すると、次に、主催者は、会議の時のみ有効な P I N コードの設定を行うために、P I N コード設定変更要求を発行し、アクセスポイント 2 0 から要求に対する受信応答を受信すると、会議期間のみ有効となる P I N コードを送信する。この新たな P I N コードを受信したアクセスポイント 2 0 は、受信した P I N コードに設定変更を行い、変更完了メッセージを、主催者の P C 4 0 へ通知する（S 6 3）。

【0 0 7 8】

主催者の P C 4 0 は、P I N コードの設定変更が完了すると、P I N コードを要求するリンクレベルによる認証の際の使用する P I N コードと、アクセスポイント 2 0 と無線端末としての P C 4 0 との間におけるリンクを確立した後に行う上位認証手順の際に、電子証明書を持っていない P C 4 0 が使用するアカウントとパスワードとが記されている参加証を作成し、参加者に配布する。

【0 0 7 9】

また、主催者は、機器操作によって会議システム管理サーバ 1 0 へアクセスを行い、今回の会議で使用するアクセスポイント 2 0 の名称、ミーティング I D 等の会議参加に必要な情報を通知し、会議で使用する共有ディスプレイ（図示せず）の画面に、それらを表示するように依頼する（S 6 4）。会議システム管理サーバ 1 0 は、上記依頼を受けると、会議で使用する共有ディスプレイの画面に、主催者から通知された上記情報を表示し、会議開催の準備を完了する。

【0 0 8 0】

一方、主催者以外の会議参加者は、会議が行われる場所で、クライアント端末を起動し（S 6 5）、先にディスプレイによって表示されているアクセスポイント 2 0 の名称から、所望のアクセスポイント 2 0 を選択し、アクセスポイント 2 0 へ、接続要求信号を発行する。

【0 0 8 1】

ここで、参加者が選択するアクセスポイント 2 0 は、参加者が持ち込んだ無線

端末の機能によって異なり、たとえば無線端末に、IEEE 802.1x等の上位認証手順処理（本実施例では上位認証手順としてIEEE 802.1xを実装した場合について記載し、以下は、802.1xサブリカント：Supplicantと記載）機能を有する場合、上位認証を行うために、リンク接続時にPINコード入力を要求しない設定のアクセスポイント20を選択し、無線端末が802.1xサブリカント機能を持たない場合、リンク接続時にリンクレベルでの認証を行うアクセスポイント20を選択する（S66）。

【0082】

ここで、802.1xサブリカント機能を持たない参加者端末が、リンクレベル認証が設定されているアクセスポイント20へ接続要求を行うと、アクセスポイント20から、リンクレベルでの認証を行うためのPINコード要求を受信する。

【0083】

そして、参加者端末は、参加証によって通知されているPINコードを送信し、リンクレベル認証が確立されると（S67）、会議システム管理サーバ10は、参加者端末の認証ルートを判定し、この参加者用に設定されたPINコードによる接続であると判断すると（S70）、会議参加者に与えられるアクセス制限をかけるIPアドレスを、参加者端末に割り当てる（S71）。

【0084】

また、802.1xサブリカント機能を有した端末が、上位認証設定されているアクセスポイント20に、リンク接続要求を発行すると、参加者端末とアクセスポイント20との間で、無線リンクが確立される。

【0085】

そして、リンクが確立されると、参加者端末は、アクセスポイント20の上位認証手順処理（ここでは、上記理由によって以下802.1xオーセンティケータ：Authenticatorと記載）機能に対して、認証要求を出力し、これを受けたアクセスポイント20は、認証に必要なIDを要求し、その後に、IEEE 802.1x手順に従って、会議システム管理サーバ10の認証サーバ機能との間で認証動作を行う（S68）。

【 0 0 8 6 】

この時に、参加者端末が電子証明書を持っていれば、会議システム管理サーバ 1 0 の認証サーバ機能によって認証され、仮に電子証明書を持っていなければ、会議システム管理サーバ 1 0 の認証サーバ機能からアカウント名とパスワードとの要求が発行される。

【 0 0 8 7 】

これを受けた参加者端末では、参加証に含まれるアカウント名とパスワードとによって、認証手順を継続させ、会議への参加認証を受ける（S 6 9）。また、これらアカウントとパスワードとを入力したときに、他のネットワーク（たとえばイントラネットやインターネット）に接続するためのアカウントとパスワードとを、参加者が持っていれば、これら正規アカウント、パスワードを入力し、認証を受けることも可能である。なお、ここで行われる ID 要求以降の認証手順は、I E E E 8 0 2 . 1 x に記載されている手順であるので、本明細書では、その手順の説明を省略する。

【 0 0 8 8 】

そして、上位認証が確立されると、会議システム管理サーバ 1 0 は、参加者端末の認証ルートを判定し、8 0 2 . 1 x 認証を受けた接続であると判断すると（S 7 0）、認証のアカウントを確認し、正規アカウント保持者であれば、会議参加者権限に加え、他のネットワークアクセスまで許可する I P アドレスを割り当て、先に配布されているアカウントによる認証者の場合には、会議参加者に与えられるアクセス制限がかかる I P アドレスを、参加者端末に与える（S 7 1）。

【 0 0 8 9 】

ここで、仮に 8 0 2 . 1 x サプリカント機能を持たない端末が、上位認証を行う設定となっているアクセスポイント 2 0 に接続した場合、無線リンク接続は、P I N コード入力なしに確立される。しかし、リンク確立後に、参加者端末では認証要求手順が行われないので、その後のアクセスを実行することができない。

【 0 0 9 0 】

一方、8 0 2 . 1 x サプリカント機能を有する参加者端末が、リンクレベル認証が設定されているアクセスポイント 2 0 に、リンク接続した場合、アクセスポ

イント 2 0 から、リンク接続時に、P I Nコード要求を受信する。そして、参加証によって通知されている P I Nコードによって、リンクレベル認証が確立されると、続いて、8 0 2 . 1 x サプリカント機能によって、上位認証要求が参加者端末から発行される。

【 0 0 9 1 】

この信号を受信したアクセスポイント 2 0 では、認証手順としてリンクレベル認証のみが有効となっているので、認証要求を無視する。そして、この参加者用に設定された P I Nコードによる接続であると、会議システム管理サーバ 1 0 が判断し、会議参加者に与えられるアクセス制限がかかる I P アドレスを、参加者端末に与える。

【 0 0 9 2 】

8 0 2 . 1 x サプリカント機能を有する参加者端末が、リンクレベル認証を設定したアクセスポイント 2 0 に接続した場合、8 0 2 . 1 x 認証を行わない例について記載しているが、リンクレベル認証の場合でも、参加者端末から上位認証要求が発行されると、上位認証手順を行い、その認証アカウントに応じた I P アドレスの割り当てを行わせるようにしてもよい。

【 0 0 9 3 】

また、認証するプロトコルのレベルに応じて、アクセスポイント 2 0 を変える例について説明したが、この構成に限定されることはなく、たとえば 1 つのアクセスポイント 2 0 に、複数の通信チャネル（独立したピコネットを形成できる構成）を持たせることによって、上記と同様の動作を実現することができる。

【 0 0 9 4 】

また、本実施例では、上位認証機能を、会議システム管理サーバ 1 0 に持たせるが、これに限定されることはなく、たとえば上位認証機能を、アクセスポイント 2 0 内に持たせ、認証情報を、会議システム管理サーバ 1 0 から取得できる手段を設けることによって、上記と同様の動作を行わせるようにしてもよい。

【 0 0 9 5 】

第 3 の実施例によれば、会議に参加する端末の認証を、複数のプロトコルレベルで行わせる手段を持たせるので、会議参加者の持ち込む端末の制限をなくすこ

とができ、また、上位認証を受けることができる機器においては、その認証機能の設定を、会議のためだけに変更することがなくなり、さらに、セキュリティレベルを保持したまま、リンクレベル認証に必要となる P I Nコード入力を省くことができ、煩雑な操作と設定とを行うことなく、会議に参加できる。

【 0 0 9 6 】

上記実施例によれば、電子メール等で予め配布される会議参加証に記載されている P I Nコードを用い、会議の参加者であるか主催者であるかを判別し、データのアクセス制限をかけるので、データの不正な改ざんを防ぐことができ、また、制限の設定を、アプリケーション上で別個に行う手間を省くことができる。

【 0 0 9 7 】

また、上位プロトコルによる認証手順に対応し、上位認証機能を有する端末については、P I Nコード入力を省くので、セキュリティを確保しつつ、非対応の端末と同様の操作で、会議に参加することができる。

【 0 0 9 8 】

なお、上記実施例において、P C 4 0 の代わりに、P D Aを使用するようにしてもよい。

【 0 0 9 9 】

【発明の効果】

本発明によれば、会議システム等のネットワークに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限を、アプリケーション上で別個に行う手間を省くことことができるという効果を奏する。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施例である無線通信システム W C 1 のブロック図である。

【図 2】

本実施例における会議システム管理サーバ 1 0 を示すブロック図である。

【図 3】

本実施例において、会議の主催者が会議に参加するまでの動作を示すフローチャートである。

【図 4】

本実施例において、会議の参加者が会議に参加するまでの動作を示すフローチャートである。

【図 5】

本実施例において、主催者がアクセスポイント 2 0 の P I N コードを変更する処理を示すシーケンス図である。

【図 6】

本実施例において、参加者が会議に参加する場合の処理を示すシーケンス図である。

【図 7】

本実施例において、主催者または参加者から送られた参加証を受信した際に、会議システム管理サーバの判別部 1 9 の動作を示すフローチャートである。

【図 8】

上記実施例において、会議システムによって制限される機能のテーブルを示す図である。

【図 9】

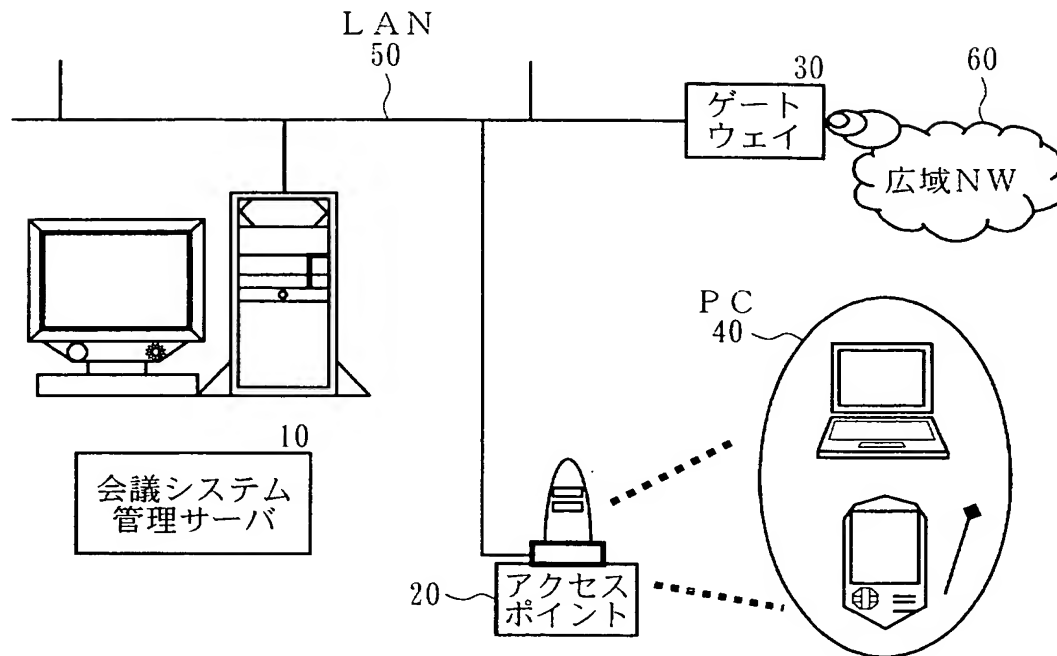
本発明の第 3 の実施例における各無線端末の操作と、その操作に従った会議システム管理サーバ 1 0 の動作を示すフローチャートである。

【符号の説明】

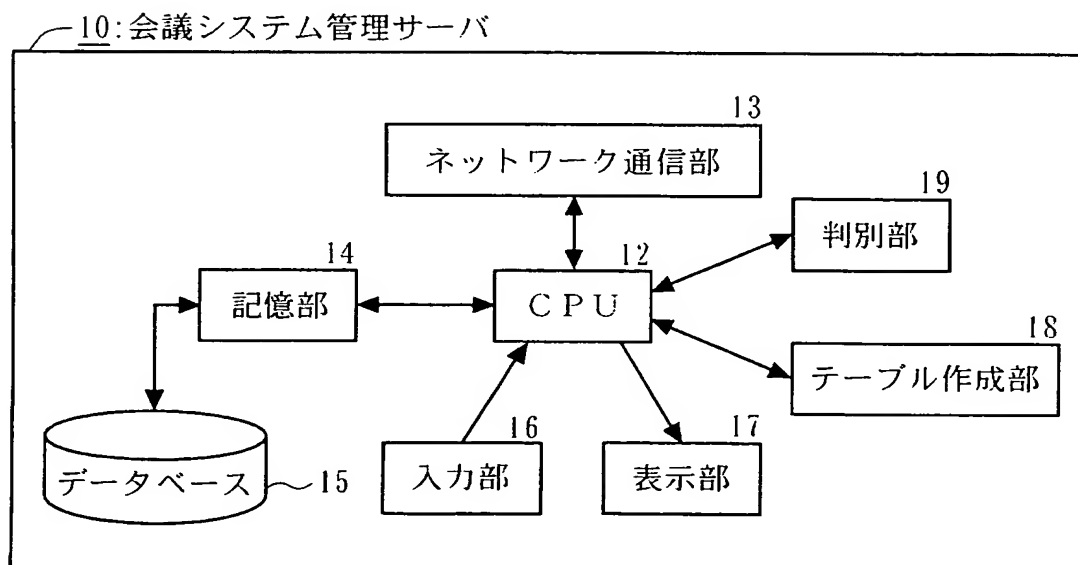
WC 1 …無線通信システム、
1 0 …会議システム管理サーバ、
2 0 …アクセスポイント、
3 0 …ゲートウェイ、
4 0 …無線端末としての P C、
5 0 …L A N。

【書類名】 図面

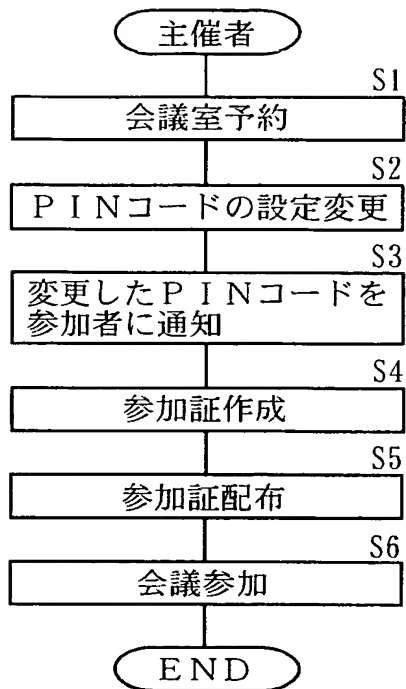
【図 1】

WC 1: 無線通信システム

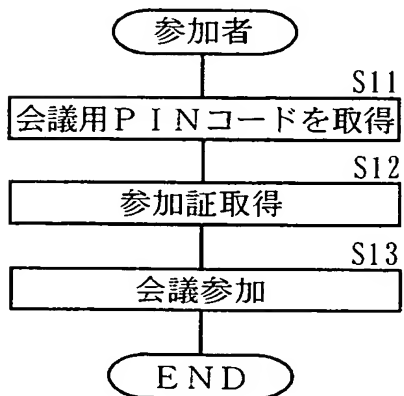
【図 2】



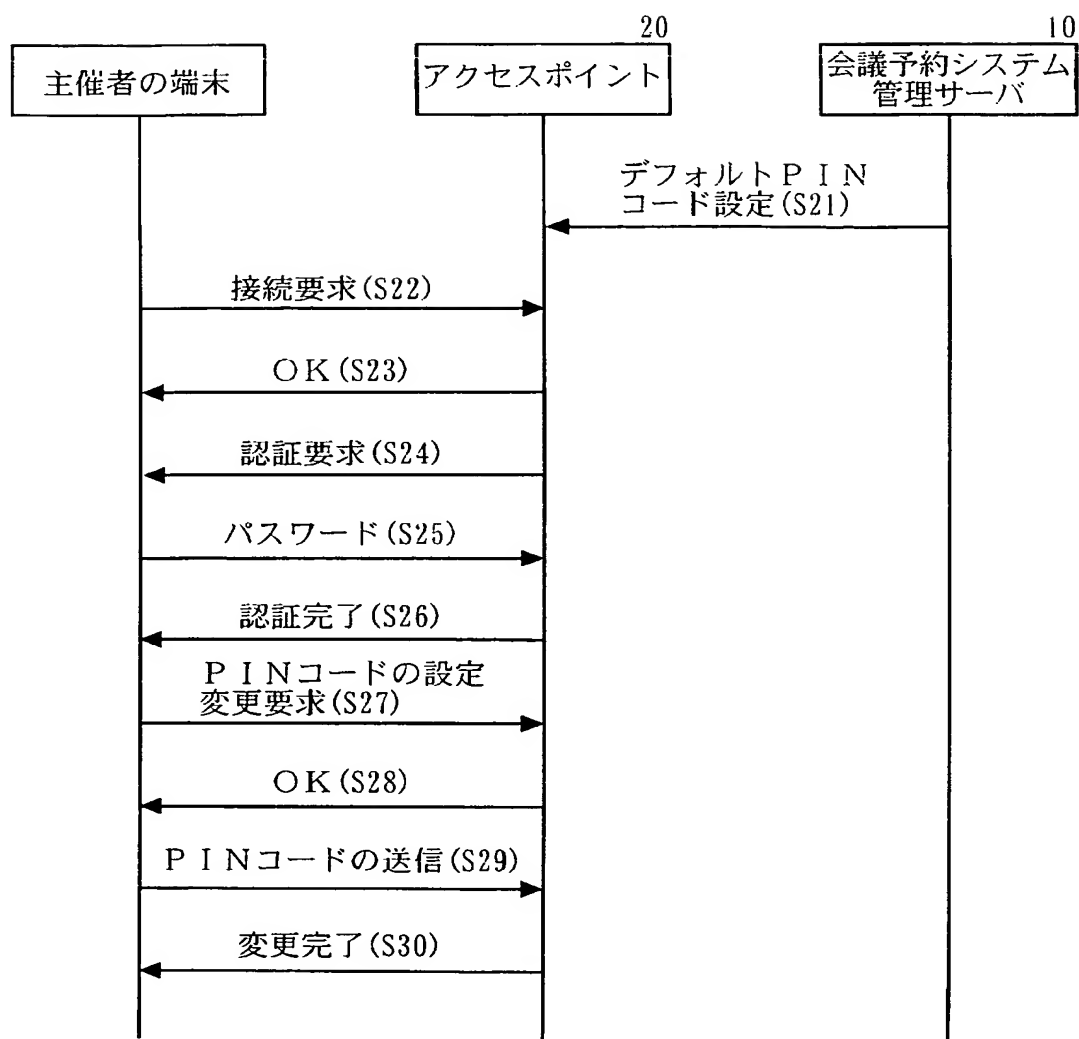
【図 3】



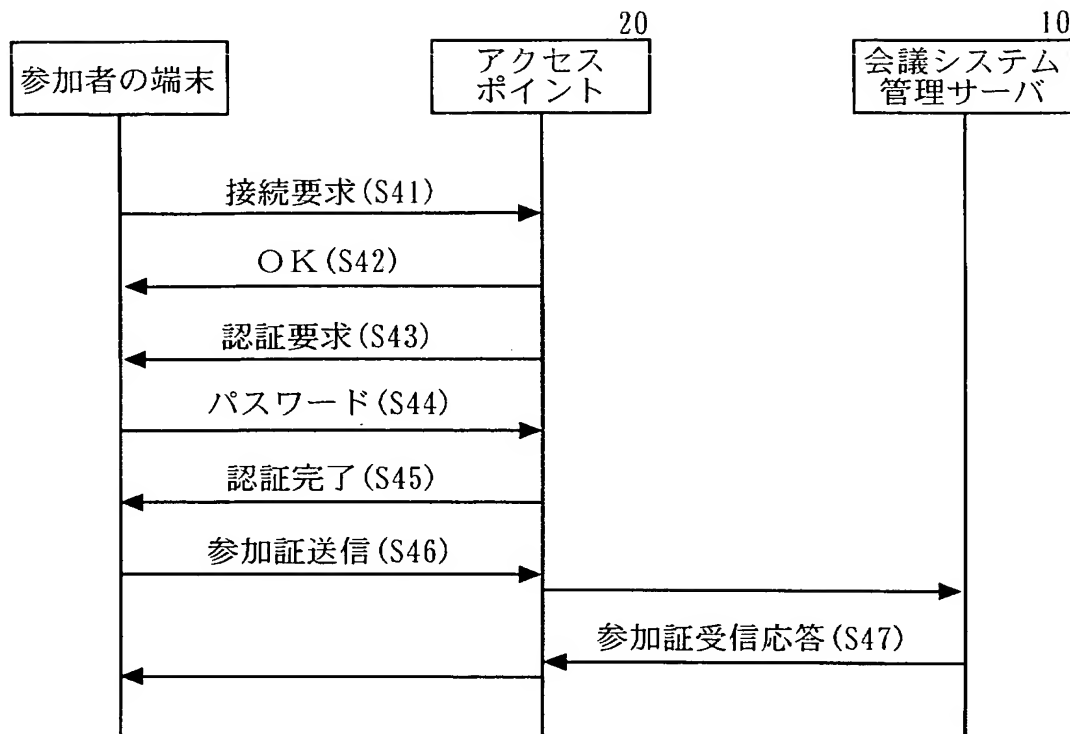
【図 4】



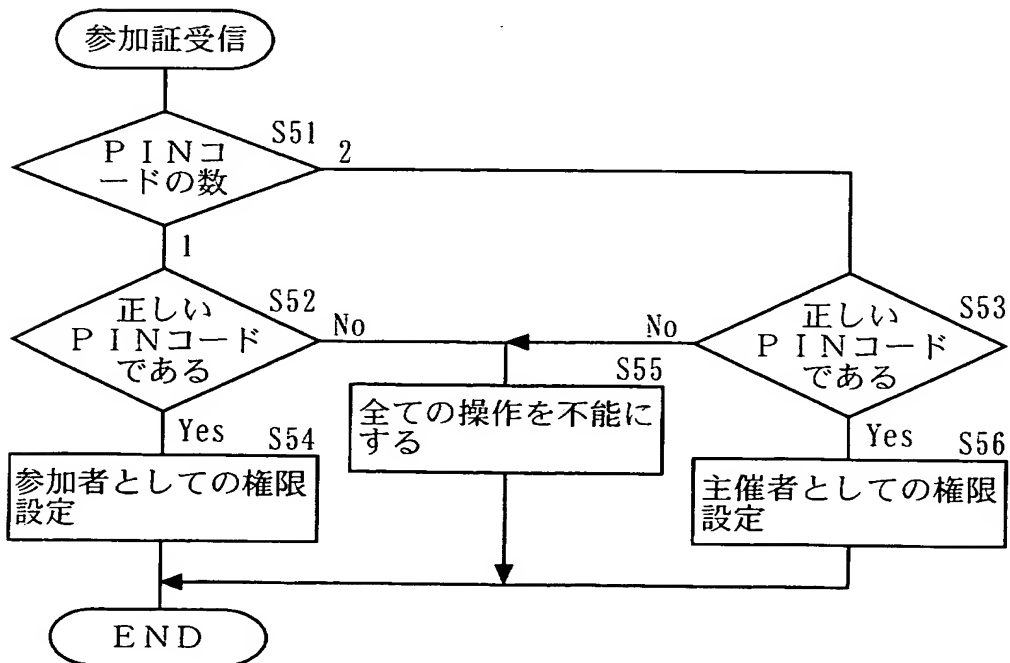
【図 5】



【図 6】



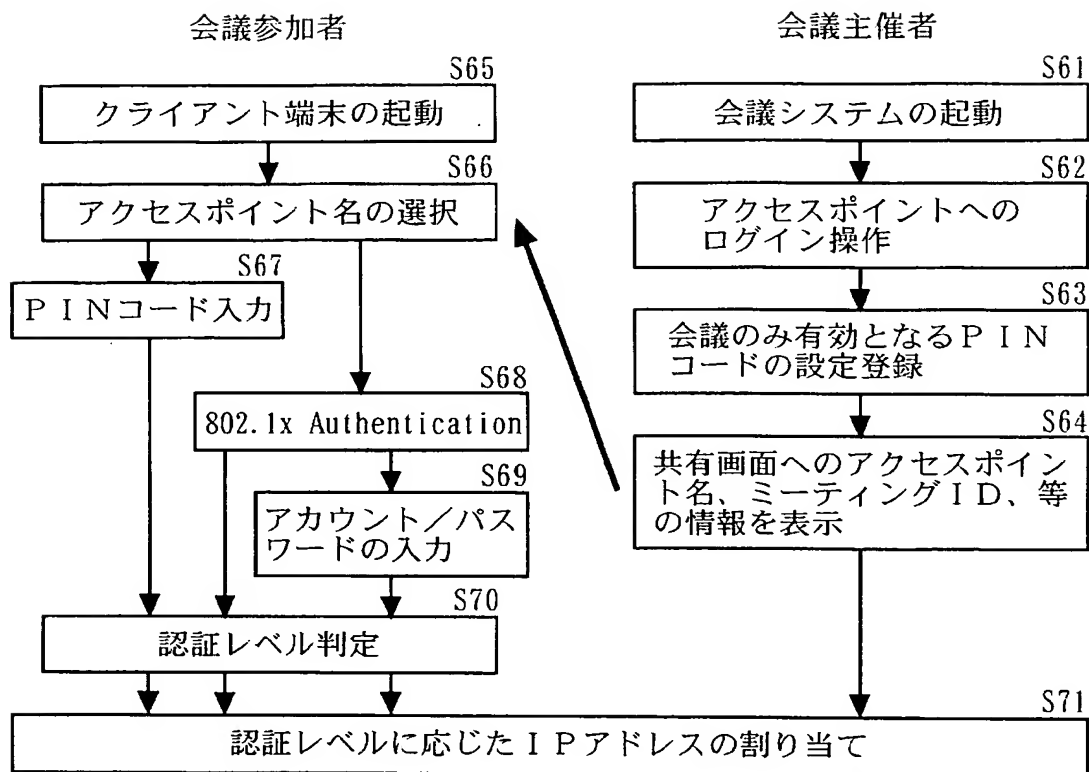
【図 7】



【図 8】

機能	主催者	参加者
ファイルの閲覧	○	○
ファイルコピー	○	×
ファイル削除	○	×
ファイル印刷	○	×
ファイル名変更	○	×
ファイル上書き	○	×
ファイル保存	○	×
ネット閲覧	○	△
I P アドレスの変更	○	×
P I N コードの変更	○	×
メール送受信	○	×

【図 9】



【書類名】 要約書

【要約】

【課題】 会議システム等のシステムに接続する機器によるデータの不正な改ざんや情報の漏洩を防ぐことができ、しかも、機能制限をアプリケーション上で別個に行う手間を省くことができる通信システムのサーバ装置を提供することを目的とするものである。

【解決手段】 会議に参加する参加者によって操作される複数の電子機器とアクセスポイントとが無線を介して接続され、上記アクセスポイントとサーバ装置とが接続されている無線通信システムにおけるサーバ装置において、認証手続きを行う際に用いる認証情報に基づいて、上記参加者の立場を判別する参加者判別手段を有することを特徴とするサーバ装置である。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 1 8 9 9 2 4
受付番号	5 0 3 0 1 1 0 0 3 2 4
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 5 年 7 月 7 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000001007
【住所又は居所】	東京都大田区下丸子 3 丁目 3 0 番 2 号
【氏名又は名称】	キャノン株式会社

【代理人】

申請人	
【識別番号】	100087446
【住所又は居所】	東京都新宿区四谷 2 丁目 4 番 1 2 号 大久保ビル 6 階
【氏名又は名称】	川久保 新一

特願 2 0 0 3 - 1 8 9 9 2 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 1 0 0 7]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都大田区下丸子 3 丁目 3 0 番 2 号

氏 名

キヤノン株式会社